Software Design, Modelling and Analysis in UML

Lecture 14: Hierarchical State Machines I

2012-12-19

Prof. Dr. Andreas Podelski, **Dr. Bernd Westphal**

Albert-Ludwigs-Universität Freiburg, Germany

Contents & Goals

Last Lecture:

- RTC-Rules: Discard, Dispatch, Commence.

This Lecture:

- **Educational Objectives:** Capabilities for following tasks/questions.
  - What does this State Machine mean? What happens if I inject this event?
  - Can you please model the following behaviour.
  - What is: initial state.
  - What does this **hierarchical** State Machine mean? What **may happen** if I inject this event?
  - What is: AND-State, OR-State, pseudo-state, entry/exit/do, final state, . . .
- **Content:**
  - Step, RTC, Divergence
  - Putting It All Together
  - Rhapsody Demo
  - Hierarchical State Machines Syntax

Step and Run-to-completion Step

Notions of Steps: The Step

Note: we call one evolution $(\sigma, \varepsilon) \xrightarrow[u]{(cons, Snd)} (\sigma', \varepsilon')$ a **step**.

Thus in our setting, **a step directly corresponds** to

one object (namely u) takes **a single transition** between regular states.

(We have to extend the concept of "single transition" for hierarchical state machines.)

That is: We're going for an interleaving semantics without true parallelism.

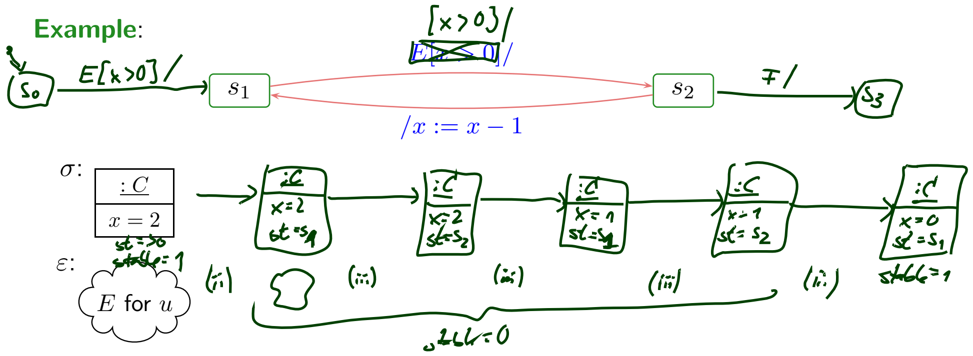
Notions of Steps: The Run-to-Completion Step

What is a **run-to-completion** step...?

- **Intuition**: a maximal sequence of steps, where the first step is a **dispatch** step and all later steps are **commence** steps.
- **Note**: one step corresponds to one transition in the state machine.

  A run-to-completion step is in general not syntacically definable — one transition may be taken multiple times during an RTC-step.

Example:



Notions of Steps: The Run-to-Completion Step Cont'd

Proposal: Let

we cannot extend the sequence while satisfying properties below

$$(\sigma_0, \varepsilon_0) \xrightarrow[u_0]{(cons_0, Snd_0)} \dots \xrightarrow[u_{n-1}]{(cons_{n-1}, Snd_{n-1})} (\sigma_n, \varepsilon_n), \quad n > 0,$$

be a finite (!), non-empty, maximal, consecutive sequence such that

$(\sigma_i, \varepsilon_i)$ and $(\sigma_{i+1}, \varepsilon_{i+1})$ are in transition relation

- object u is alive in σ_0,
- $u_0 = u$ and $(cons_0, Snd_0)$ indicates dispatching to u, i.e. $cons = \{(u, \vec{v} \mapsto \vec{d})\}$,
- there are no receptions by u in between, i.e.

$$cons_i \cap \{u\} \times Evs(\mathscr{E}, \mathscr{D}) = \emptyset, i > 1,$$

- $u_{n-1} = u$ and u is stable only in σ_0 and σ_n, i.e.

$$\sigma_0(u)(stable) = \sigma_n(u)(stable) = 1 \text{ and } \sigma_i(u)(stable) = 0 \text{ for } 0 < i < n,$$

Let $0 = k_1 < k_2 < \dots < k_N = n$ be the maximal sequence of indices such that $u_{k_i} = u$ for $1 \leq i \leq N$. Then we call the sequence

$$(\sigma_0(u) =) \quad \sigma_{k_1}(u), \sigma_{k_2}(u) \dots, \sigma_{k_N}(u) \quad (= \sigma_{n-1}(u))$$

a (!) **run-to-completion computation** of u (from (local) configuration $\sigma_0(u)$).

Divergence

We say, object u **can diverge** on reception $cons$ from (local) configuration $\sigma_0(u)$ if and only if there is an infinite, consecutive sequence

$$(\sigma_0, \varepsilon_0) \xrightarrow[u]{(cons_0, Snd_0)} (\sigma_1, \varepsilon_1) \xrightarrow[u]{(cons_1, Snd_1)} \dots$$

such that u doesn't become stable again.

- **Note**: disappearance of object not considered in the definitions.
  By the current definitions, it's ~~neither~~ divergence ~~nor~~ an RTC-step.
  but not

Run-to-Completion Step: Discussion.

What people may **dislike** on our definition of RTC-step is that it takes a **global** and **non-compositional** view. That is:

- In the projection onto a single object we still **see** the effect of interaction with other objects.
- Adding classes (or even objects) may change the divergence behaviour of existing ones.
- Compositional would be: the behaviour of a set of objects is determined by the behaviour of each object "in isolation".
  Our semantics and notion of RTC-step doesn't have this (often desired) property.

Can we give (syntactical) criteria such that any global run-to-completion step is an interleaving of local ones?

Maybe: **Strict interfaces**. (*Proof left as exercise...*)

- **(A)**: Refer to private features only via "self".
  (Recall that other objects of the same class can modify private attributes.)
- **(B)**: Let objects only communicate by events, i.e.
  don't let them modify each other's local state via links **at all**.

Putting It All Together

The Missing Piece: Initial States

Recall: a labelled transition system is $(S, \rightarrow, S_0)$. We **have**

- S: system configurations (σ, ε)
- $\rightarrow$: labelled transition relation $(\sigma, \varepsilon) \xrightarrow[u]{(cons, Snd)} (\sigma', \varepsilon')$.

Wanted: initial states S_0.

Proposal:
Require a (finite) set of **object diagrams** $\mathcal{OD}$ as part of a UML model

$$(\mathscr{CD}, \mathscr{SM}, \mathscr{OD}).$$

And set

$$S_0 = \{(\sigma, \varepsilon) \mid \sigma \in G^{-1}(\mathcal{OD}), \mathcal{OD} \in \mathscr{OD}, \varepsilon \text{ empty}\}.$$

Other Approach: (used by Rhapsody tool) multiplicity of classes.
We can read that as an abbreviation for an object diagram.

Semantics of UML Model — So Far

The **semantics** of the **UML model**

$$\mathcal{M} = (\mathscr{CD}, \mathscr{SM}, \mathscr{OD})$$

where

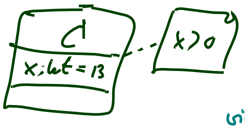
- some classes in $\mathscr{CD}$ are stereotyped as ‘signal’ (standard), some signals and attributes are stereotyped as ‘external’ (non-standard),
- there is a 1-to-1 relation between classes and state machines,
- $\mathscr{OD}$ is a set of object diagrams over $\mathscr{CD}$,

is the **transition system** $(S, \to, S_0)$ constructed on the previous slide.

S: system configurations, by $\mathscr{CD}$ — $\to$: defined by rules (i)-(v) on $\mathscr{SM}$ — S_0: given by $\mathscr{OD}$

The **computations of** $\mathcal{M}$ are the computations of $(S, \to, S_0)$. (starting in one initial system configuration)

OCL Constraints and Behaviour

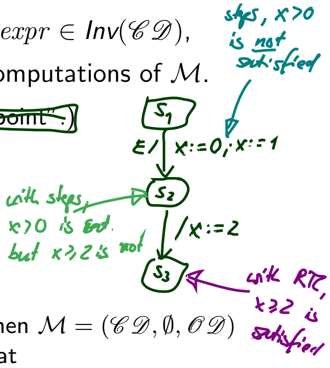


- Let $\mathcal{M} = (\mathscr{CD}, \mathscr{SM}, \mathscr{OD})$ be a UML model.
- We call $\mathcal{M}$ **consistent** iff, for each OCL constraint $expr \in Inv(\mathscr{CD})$,

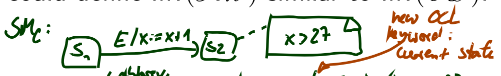
  $\sigma \models expr$ for each “reasonable point” (σ, ε) of computations of $\mathcal{M}$.

~~(Cf. exercises and tutorial for discussion of “reasonable point”.)~~

Our choice: “by step”, consider each (σ, ε) in computation.



Note: we could define $Inv(\mathscr{SM})$ similar to $Inv(\mathscr{CD})$.



new OCL keyword: current state

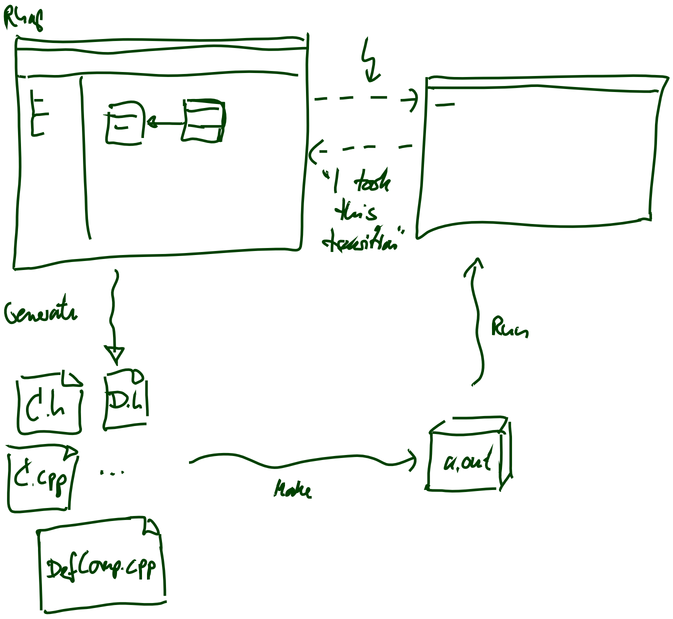
abbrev. context C inv : $\underline{st} = S_2$ implies $x > 27$

Pragmatics:

- In **UML-as-blueprint mode**, if $\mathscr{SM}$ doesn’t exist yet, then $\mathcal{M} = (\mathscr{CD}, \emptyset, \mathscr{OD})$ is typically asking the developer to provide $\mathscr{SM}$ such that $\mathcal{M}' = (\mathscr{CD}, \mathscr{SM}, \mathscr{OD})$ is consistent.

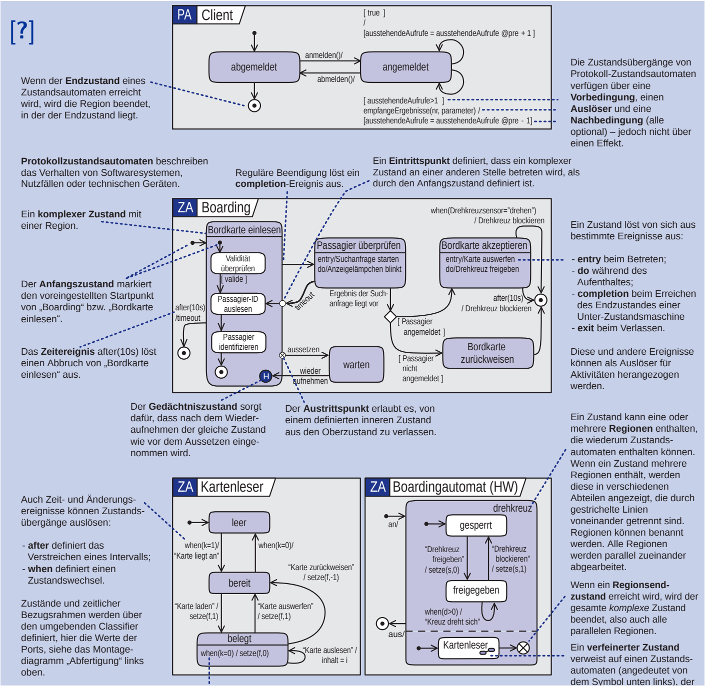
  If the developer makes a mistake, then $\mathcal{M}'$ is inconsistent.
- **Not common**: if $\mathscr{SM}$ is given, then constraints are also considered when choosing transitions in the RTC-algorithm. In other words: even in presence of mistakes, the $\mathscr{SM}$ never move to inconsistent configurations.

Contemporary UML Modelling Tools



Hierarchical State Machines

UML State-Machines: What do we have to cover?



[?]

Wenn der **Endzustand** eines Zustandsautomaten erreicht wird, wird die Region beendet, in der der Endzustand liegt.

Die Zustandsübergänge von Protokoll-Zustandsautomaten verfügen über eine **Vorbedingung**, einen **Auslöser** und eine **Nachbedingung** (alle optional) – jedoch nicht über einen Effekt.

Protokollzustandsautomaten beschreiben das Verhalten von Softwaresystemen, Nutzfällen oder technischen Geräten.

Reguläre Beendigung löst ein **completion**-Ereignis aus.

Ein **Eintrittspunkt** definiert, dass ein komplexer Zustand an einer anderen Stelle betreten wird, als durch den Anfangszustand definiert ist.

Ein **komplexer Zustand** mit einer Region.

Der **Anfangszustand** markiert den voreingestellten Startpunkt von „Boarding“ bzw. „Bordkarte einlesen“.

Das **Zeitereignis** after(10s) löst einen Abbruch von „Bordkarte einlesen“ aus.

Ein Zustand löst von sich aus bestimmte Ereignisse aus:

- **entry** beim Betreten;
- **do** während des Aufenthaltes;
- **completion** beim Erreichen des Endzustandes einer Unter-Zustandsmaschine
- **exit** beim Verlassen.

Diese und andere Ereignisse können als Auslöser für Aktivitäten herangezogen werden.

Der **Gedächtniszustand** sorgt dafür, dass nach dem Wiederaufnehmen der gleiche Zustand wie vor dem Aussetzen eingenommen wird.

Der **Austrittspunkt** erlaubt es, von einem definierten inneren Zustand aus den Oberzustand zu verlassen.

Ein Zustand kann eine oder mehrere **Regionen** enthalten, die wiederum Zustandsautomaten enthalten können. Wenn ein Zustand mehrere Regionen enthält, werden diese in verschiedenen Abteilen angezeigt, die durch gestrichelte Linien voneinander getrennt sind. Regionen können benannt werden. Alle Regionen werden parallel zueinander abgearbeitet.

Auch Zeit- und Änderungsereignisse können Zustandsübergänge auslösen:

- **after** definiert das Verstreichen eines Intervalls;
- **when** definiert einen Zustandswechsel.

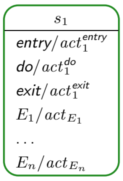
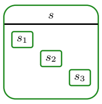
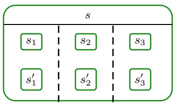
Zustände und zeitlicher Bezugsrahmen werden über den umgebenden Classifier definiert, hier die Werte der Ports, siehe das Montagediagramm „Abfertigung“ links oben.

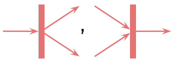
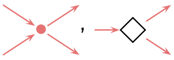
Wenn ein **Regionsendzustand** erreicht wird, wird der gesamte *komplexe* Zustand beendet, also auch alle parallelen Regionen.

Ein **verfeinerter Zustand** verweist auf einen Zustandsautomaten (angedeutet von dem Symbol unten links), der

The Full Story

UML distinguishes the following **kinds of states**:

	example
simple state	
final state	◉
composite state	
OR	
AND	

	example
pseudo-state	
initial	●
(shallow) history	Ⓗ
deep history	H*
fork/join	
junction, choice	
entry point	○
exit point	⊗
terminate	×
submachine state	$\boxed{S : s}$

Representing All Kinds of States

- **Until now**:

$$(S, s_0, \rightarrow), \quad s_0 \in S, \rightarrow \subseteq S \times (\mathscr{E} \cup \{\_\}) \times Expr_{\mathscr{S}} \times Act_{\mathscr{S}} \times S$$

Representing All Kinds of States

- **Until now**:

$$(S, s_0, \to), \quad s_0 \in S, \to \; \subseteq S \times (\mathscr{E} \cup \{\_\}) \times \mathit{Expr}_{\mathscr{S}} \times \mathit{Act}_{\mathscr{S}} \times S$$

- **From now on**: (**hierarchical**) **state machines**

$$(S, \mathit{kind}, \mathit{region}, \to, \psi, \mathit{annot})$$

Representing All Kinds of States

- **Until now**:

$$(S, s_0, \to), \quad s_0 \in S, \to \; \subseteq S \times (\mathscr{E} \cup \{\_\}) \times \mathit{Expr}_{\mathscr{S}} \times \mathit{Act}_{\mathscr{S}} \times S$$

- **From now on**: (**hierarchical**) **state machines**

$$(S, \mathit{kind}, \mathit{region}, \to, \psi, \mathit{annot})$$

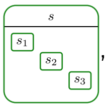
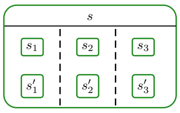
where

- $S \supseteq \{top\}$ is a finite set of states **(as before)**,
- $\mathit{kind} : S \to \{$*st*, *init*, *fin*, *shist*, *dhist*, *fork*, *join*, *junc*, *choi*, *ent*, *exi*, *term*$\}$ is a function which labels states with their **kind**, **(new)**
- $\mathit{region} : S \to 2^{2^S}$ is a function which characterises the **regions** of a state, **(new)**
- $\to$ is a set of transitions, **(changed)**
- $\psi : (\to) \to 2^S \times 2^S$ is an **incidence function**, and **(new)**
- $\mathit{annot} : (\to) \to (\mathscr{E} \cup \{\_\}) \times \mathit{Expr}_{\mathscr{S}} \times \mathit{Act}_{\mathscr{S}}$ provides an annotation for each transition. **(new)**

(s_0 is then redundant — replaced by proper state (!) of kind '*init*'.)

From UML to Hierarchical State Machines: By Example

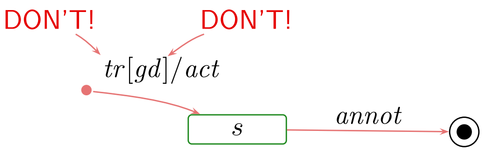
$(S, kind, region, \to, \psi, annot)$

	example	$\in S$	$kind$	$region$
simple state	$\boxed{s}$	s	*st*	$\emptyset$
final state	◉	q	*fin*	$\emptyset$
composite state				
OR	,	s	*st*	$\{\{s_1, s_2, s_3\}\}$
AND		s	*st*	$\{\{s_1, s'_1\}, \{s_2, s'_2\}, \{s_3, s'_3\}\}$
submachine state	(later) -	-	-	
pseudo-state	●, . . .	q	*init*, . . .	$\emptyset$

region

$\underbrace{\in S \quad kind}_{(s, kind(s)) \text{ for short}}$

From UML to Hierarchical State Machines: By Example



... translates to $(S, kind, region, \to, \psi, annot) =$

$$(\underbrace{\{(top, st), (s_1, init), (s, st), (s_2, fin)\}}_{S, kind},$$

$$\underbrace{\{top \mapsto \{\{s_1, s, s_2\}\}, s_1 \mapsto \emptyset, s \mapsto \emptyset, s_2 \mapsto \emptyset\}}_{region},$$

$$\underbrace{\{t_1, t_2\}}_{\to}, \quad \underbrace{\{t_1 \mapsto (\{s_1\}, \{s\}), t_2 \mapsto (\{s\}, \{s_2\})\}}_{\psi},$$

$$\underbrace{\{t_1 \mapsto (tr, gd, act), t_2 \mapsto annot\}}_{annot})$$

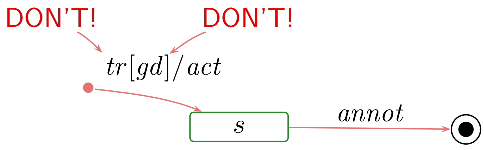
Well-Formedness: Regions (follows from diagram)

	$\in S$	*kind*	$\mathit{region} \subseteq 2^S, S_i \subseteq S$	$\mathit{child} \subseteq S$
simple state	s	*st*	$\emptyset$	$\emptyset$
final state	s	*fin*	$\emptyset$	$\emptyset$
composite state	s	*st*	$\{S_1, \dots, S_n\}, n \geq 1$	$S_1 \cup \dots \cup S_n$
pseudo-state	s	*init*, ...	$\emptyset$	$\emptyset$
implicit top state	top	*st*	$\{S_1\}$	S_1

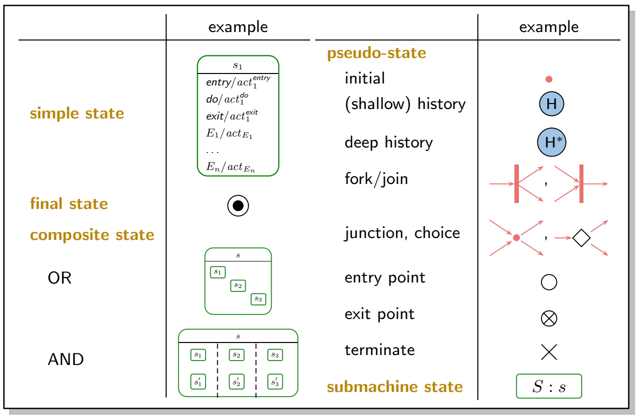
- Each state (except for top) lies in exactly one region,
- States $s \in S$ with $\mathit{kind}(s) =$ *st* **may comprise** regions.
  - No region: simple state.
  - One region: OR-state.
  - Two or more regions: AND-state.
- Final and pseudo states **don't comprise** regions.
- The region function induces a **child** function.

Well-Formedness: Initial State (requirement on diagram)

- Each non-empty region has a reasonable initial state and at least one transition from there, i.e.
  - for each $s \in S$ with $\mathit{region}(s) = \{S_1, \dots, S_n\}$, $n \geq 1$, for each $1 \leq i \leq n$,
  - there exists exactly one initial pseudo-state $(s_1^i, \mathit{init}) \in S_i$ and at least one transition $t \in \longrightarrow$ with s_1^i as source,
  - and such transition's target s_2^i is in S_i, and (**for simplicity!**) $\mathit{kind}(s_2^i) =$ *st*, and $\mathit{annot}(t) = (\_, \mathit{true}, \mathit{act})$.
- No ingoing transitions to initial states.
- No outgoing transitions from final states.
- Recall:



Plan

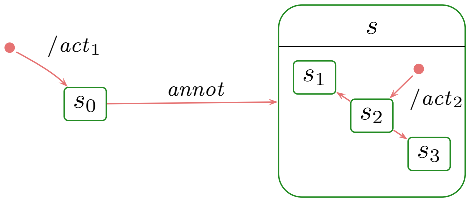


	example		example
		pseudo-state	
		initial	●
simple state	s_1 entry/act_1^{entry} do/act_1^{do} exit/act_1^{exit} E_1/act_{E_1} … E_n/act_{E_n}	(shallow) history	H
		deep history	H*
		fork/join	,
final state	◉		
composite state		junction, choice	,
OR	s s_1 s_2 s_3	entry point	○
		exit point	⊗
AND	s s_1 s_2 s_3 s_1' s_2' s_3'	terminate	×
		submachine state	$S : s$

- Initial pseudostate, final state.
- Composite states.
- Entry/do/exit actions, internal transitions.
- History and other pseudostates, the rest.

Initial Pseudostates and Final States

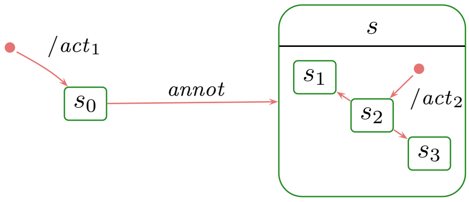
Initial Pseudostate



Principle:

- when entering a region **without** a specific destination state,
- then go to a state which is destination of an initiation transition,
- execute the action of the chosen initiation transitions **between** exit and entry actions.

Initial Pseudostate



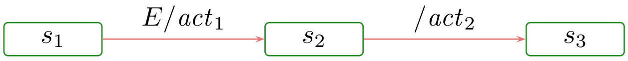
Principle:

- when entering a region **without** a specific destination state,
- then go to a state which is destination of an initiation transition,
- execute the action of the chosen initiation transitions **between** exit and entry actions.

Special case: the region of top.

- If class C has a state-machine, then “create-C transformer” is the concatenation of
  - the transformer of the “constructor” of C (here not introduced explicitly) and
  - a transformer corresponding to one initiation transition of the top region.

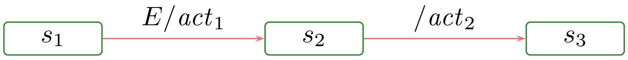
Towards Final States: Completion of States



- Transitions without trigger can **conceptionally** be viewed as being sensitive for the "completion event".
- Dispatching (here: E) **can then alternatively** be **viewed** as

---

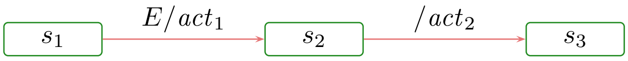
Towards Final States: Completion of States



- Transitions without trigger can **conceptionally** be viewed as being sensitive for the "completion event".
- Dispatching (here: E) **can then alternatively** be **viewed** as

  (i) fetch event (here: E) from the ether,

Towards Final States: Completion of States

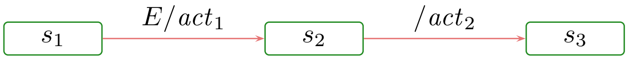


- Transitions without trigger can **conceptionally** be viewed as being sensitive for the "completion event".
- Dispatching (here: E) **can then alternatively** be **viewed** as

  (i) fetch event (here: E) from the ether,

  (ii) take an enabled transition (here: to s_2),

Towards Final States: Completion of States



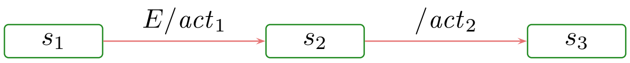
- Transitions without trigger can **conceptionally** be viewed as being sensitive for the "completion event".
- Dispatching (here: E) **can then alternatively** be **viewed** as

  (i) fetch event (here: E) from the ether,

  (ii) take an enabled transition (here: to s_2),

  (iii) remove event from the ether,

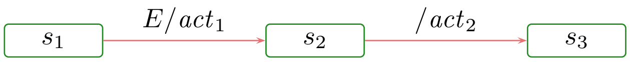
Towards Final States: Completion of States



- Transitions without trigger can **conceptionally** be viewed as being sensitive for the "completion event".
- Dispatching (here: E) **can then alternatively** be **viewed** as
  - (i) fetch event (here: E) from the ether,
  - (ii) take an enabled transition (here: to s_2),
  - (iii) remove event from the ether,
  - (iv) after having finished entry and do action of current state (here: s_2) — the state is then called **completed** —,

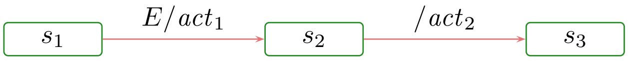
---

Towards Final States: Completion of States



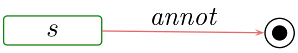
- Transitions without trigger can **conceptionally** be viewed as being sensitive for the "completion event".
- Dispatching (here: E) **can then alternatively** be **viewed** as
  - (i) fetch event (here: E) from the ether,
  - (ii) take an enabled transition (here: to s_2),
  - (iii) remove event from the ether,
  - (iv) after having finished entry and do action of current state (here: s_2) — the state is then called **completed** —,
  - (v) raise a **completion event** — with strict priority over events from ether!

Towards Final States: Completion of States



- Transitions without trigger can **conceptionally** be viewed as being sensitive for the “completion event”.
- Dispatching (here: E) **can then alternatively** be **viewed** as
  - (i) fetch event (here: E) from the ether,
  - (ii) take an enabled transition (here: to s_2),
  - (iii) remove event from the ether,
  - (iv) after having finished entry and do action of current state (here: s_2) — the state is then called **completed** —,
  - (v) raise a **completion event** — with strict priority over events from ether!
  - (vi) if there is a transition enabled which is sensitive for the completion event,
    - then take it (here: (s_2, s_3)).
    - otherwise become stable.

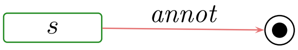
Final States



- If
  - a step of object u moves u into a final state (s, fin), and
  - all sibling regions are in a final state,

  then (conceptionally) a completion event for the current composite state s is raised.

Final States



- If
  - a step of object u moves u into a final state (s, fin), and
  - all sibling regions are in a final state,

  then (conceptionally) a completion event for the current composite state s is raised.
- If there is a transition of a **parent state** (i.e., inverse of $child$) of s enabled which is sensitive for the completion event,
  - then take that transition,
  - otherwise kill u

  $\rightsquigarrow$ adjust $(2.)$ and $(3.)$ in the semantics accordingly

---

Final States

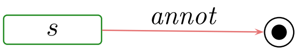
- If
  - a step of object u moves u into a final state (s, fin), and
  - all sibling regions are in a final state,

  then (conceptionally) a completion event for the current composite state s is raised.
- If there is a transition of a **parent state** (i.e., inverse of $child$) of s enabled which is sensitive for the completion event,
  - then take that transition,
  - otherwise kill u

  $\rightsquigarrow$ adjust $(2.)$ and $(3.)$ in the semantics accordingly

- **One consequence**: u never survives reaching a state (s, fin) with $s \in child(top)$.

Final States



- If
  - a step of object u moves u into a final state (s, fin), and
  - all sibling regions are in a final state,

  then (conceptionally) a completion event for the current composite state s is raised.
- If there is a transition of a **parent state** (i.e., inverse of $child$) of s enabled which is sensitive for the completion event,
  - then take that transition,
  - otherwise kill u

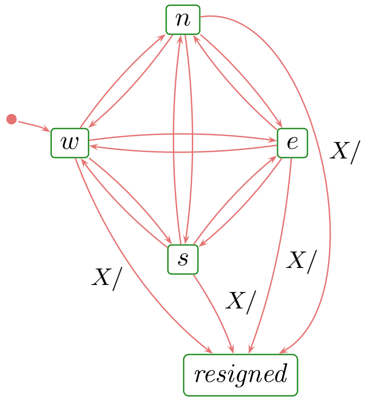
  ⇝ adjust $(2.)$ and $(3.)$ in the semantics accordingly
- **One consequence**: u never survives reaching a state (s, fin) with $s \in child(top)$.
- **Now:** in Core State Machines, there is no parent state.
- **Later:** in Hierarchical ones, there may be one.

Composite States

(formalisation follows [?])

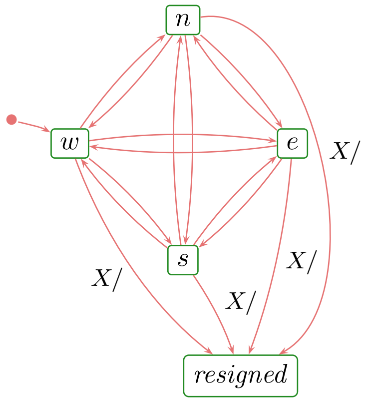
Composite States

- In a sense, composite states are about **abbreviation**, **structuring**, and **avoiding redundancy**.
- Idea: in Tron, for the Player's Statemachine, instead of

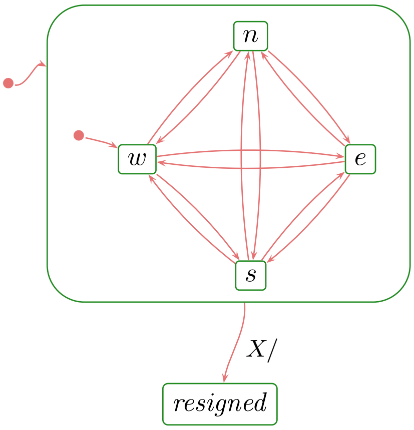


Composite States

- In a sense, composite states are about **abbreviation**, **structuring**, and **avoiding redundancy**.
- Idea: in Tron, for the Player's Statemachine, instead of

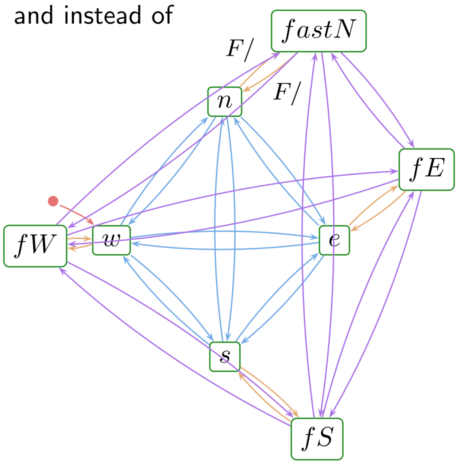


write



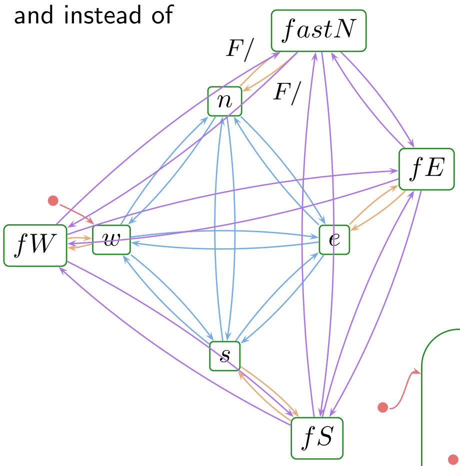
Composite States

and instead of

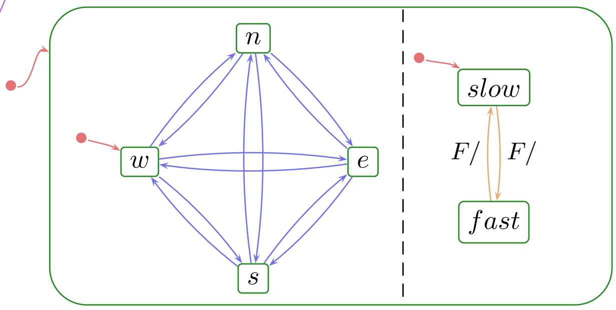


Composite States

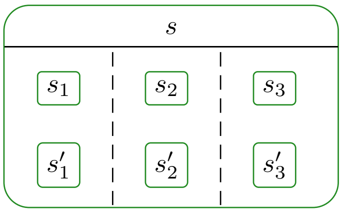
and instead of



write



Recall: Syntax



translates to

$$(\underbrace{\{(top, \mathsf{st}), (s, \mathsf{st}), (s_1, \mathsf{st})(s_1', \mathsf{st})(s_2, \mathsf{st})(s_2', \mathsf{st})(s_3, \mathsf{st})(s_3', \mathsf{st})\}}_{S, kind},$$

$$\underbrace{\{top \mapsto \{s\}, s \mapsto \{\{s_1, s_1'\}, \{s_2, s_2'\}, \{s_3, s_3'\}\}, s_1 \mapsto \emptyset, s_1' \mapsto \emptyset, \dots\}}_{region},$$

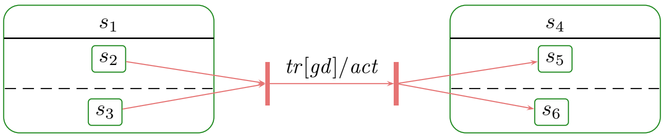
$$\to, \psi, annot)$$

Syntax: Fork/Join

- For brevity, we always consider transitions with (possibly) multiple sources and targets, i.e.

$$\psi : (\to) \to (2^S \setminus \emptyset) \times (2^S \setminus \emptyset)$$

- For instance,

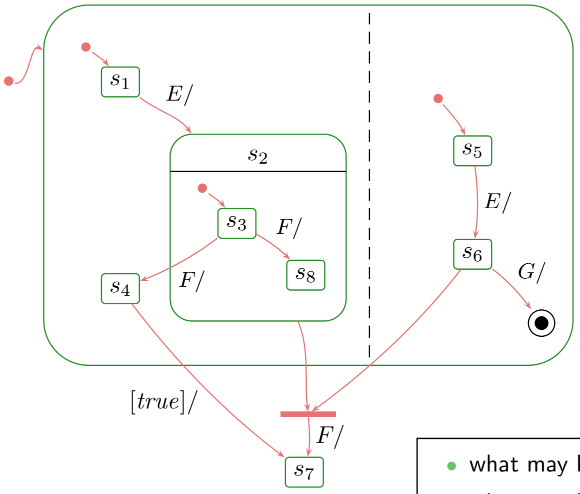


translates to

$$(S, kind, region, \underbrace{\{t_1\}}_{\to}, \underbrace{\{t_1 \mapsto (\{s_2, s_3\}, \{s_5, s_6\})\}}_{\psi}, \underbrace{\{t_1 \mapsto (tr, gd, act)\}}_{annot})$$

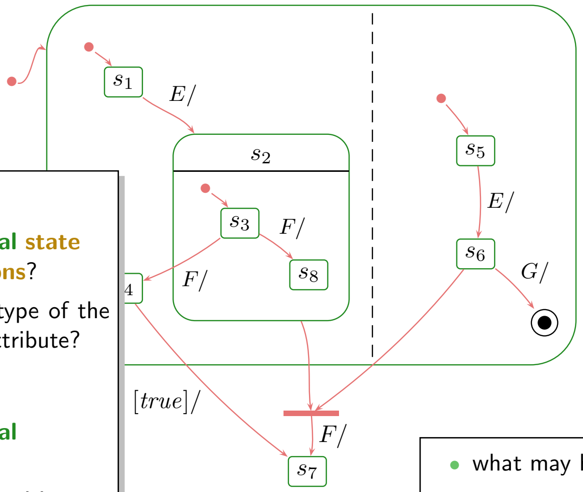
- Naming convention: $\psi(t) = (source(t), target(t))$.

Composite States: Blessing or Curse?



- what may happen on E?
- what may happen on E, F?
- can E, G kill the object?
- …

Composite States: Blessing or Curse?



States:

- what are **legal state configurations**?
- what is the type of the implicit st attribute?

Transitions:

- what are **legal** transitions?
- when is a transition enabled?
- what effects do transitions have?

- what may happen on E?
- what may happen on E, F?
- can E, G kill the object?
- …

State Configuration

- The type of st is from now on **a set of** states, i.e. $st : 2^S$
- A set $S_1 \subseteq S$ is called (**legal**) **state configurations** if and only if
  - $top \in S_1$, and
  - with each state $s \in S_1$ that has a non-empty region $\emptyset \neq R \in region(s)$, exactly one (non pseudo-state) child of s is in S_1, i.e.

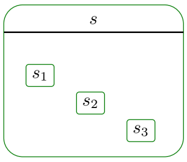
$$|\{s \in R \mid kind(s) \in \{\mathit{st}, \mathit{fin}\}\} \cap S_1| = 1.$$

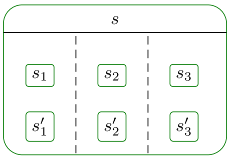
State Configuration

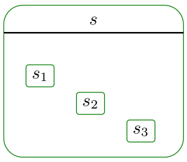
- The type of st is from now on **a set of** states, i.e. $st : 2^S$
- A set $S_1 \subseteq S$ is called (**legal**) **state configurations** if and only if
  - $top \in S_1$, and
  - with each state $s \in S_1$ that has a non-empty region $\emptyset \neq R \in region(s)$, exactly one (non pseudo-state) child of s is in S_1, i.e.

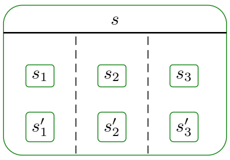
$$|\{s \in R \mid kind(s) \in \{\mathit{st}, \mathit{fin}\}\} \cap S_1| = 1.$$

- **Examples**:









A Partial Order on States

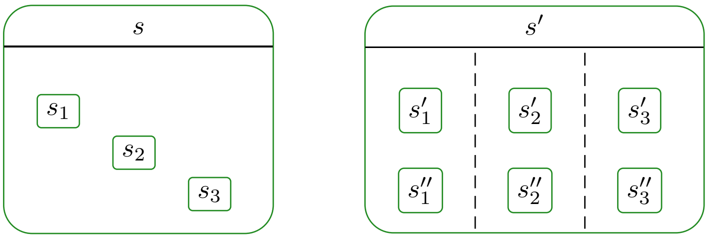
The substate- (or **child**-) relation **induces** a **partial order on states**:

- $top \le s$, for all $s \in S$,
- $s \le s'$, for all $s' \in child(s)$,
- transitive, reflexive, antisymmetric,
- $s' \le s$ and $s'' \le s$ implies $s' \le s''$ or $s'' \le s'$.

A Partial Order on States

The substate- (or **child**-) relation **induces** a **partial order on states**:

- $top \le s$, for all $s \in S$,
- $s \le s'$, for all $s' \in child(s)$,
- transitive, reflexive, antisymmetric,
- $s' \le s$ and $s'' \le s$ implies $s' \le s''$ or $s'' \le s'$.



Least Common Ancestor and Ting

- The **least common ancestor** is the function $lca : 2^S \rightarrow S$ such that
  - The states in S_1 are (transitive) children of $lca(S_1)$, i.e.

$$lca(S_1) \leq s, \text{ for all} s \in S_1 \subseteq S,$$

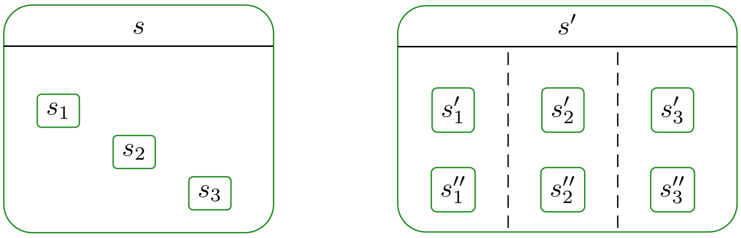
  - $lca(S_1)$ is minimal, i.e. if $\hat{s} \leq s$ for all $s \in S_1$, then $\hat{s} \leq lca(S_1)$
- **Note**: $lca(S_1)$ exists for all $S_1 \subseteq S$ (last candidate: top).

Least Common Ancestor and Ting

- The **least common ancestor** is the function $lca : 2^S \rightarrow S$ such that
  - The states in S_1 are (transitive) children of $lca(S_1)$, i.e.

$$lca(S_1) \leq s, \text{ for all} s \in S_1 \subseteq S,$$

  - $lca(S_1)$ is minimal, i.e. if $\hat{s} \leq s$ for all $s \in S_1$, then $\hat{s} \leq lca(S_1)$
- **Note**: $lca(S_1)$ exists for all $S_1 \subseteq S$ (last candidate: top).



Least Common Ancestor and Ting

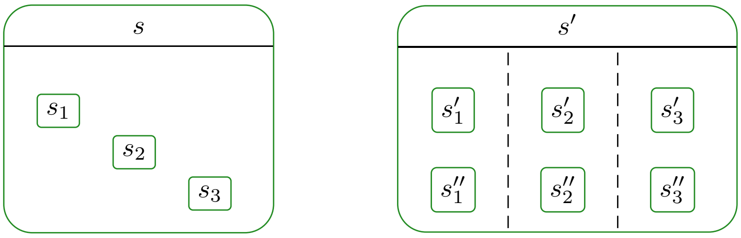
- Two states $s_1, s_2 \in S$ are called **orthogonal**, denoted $s_1 \perp s_2$, if and only if
  - they are unordered, i.e. $s_1 \not\leq s_2$ and $s_2 \not\leq s_1$, and
  - they live in different regions of an AND-state, i.e.

$$\exists\, s, \mathit{region}(s) = \{S_1, \ldots, S_n\}, 1 \leq i \neq j \leq n : s_1 \in \mathit{child}(S_i) \wedge s_2 \in \mathit{child}(S_j),$$

Least Common Ancestor and Ting

- Two states $s_1, s_2 \in S$ are called **orthogonal**, denoted $s_1 \perp s_2$, if and only if
  - they are unordered, i.e. $s_1 \not\leq s_2$ and $s_2 \not\leq s_1$, and
  - they live in different regions of an AND-state, i.e.

$$\exists\, s, \mathit{region}(s) = \{S_1, \ldots, S_n\}, 1 \leq i \neq j \leq n : s_1 \in \mathit{child}(S_i) \wedge s_2 \in \mathit{child}(S_j),$$

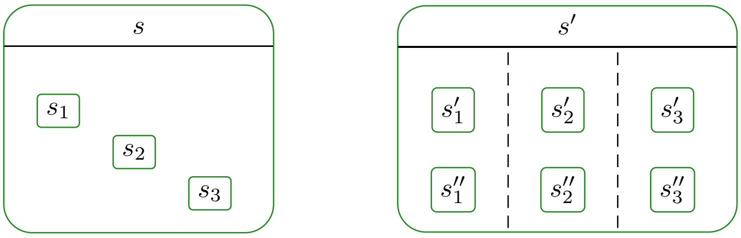


Least Common Ancestor and Ting

- A set of states $S_1 \subseteq S$ is called **consistent**, denoted by $\downarrow S_1$, if and only if for each $s, s' \in S_1$,
  - $s \leq s'$,
  - $s' \leq s$, or
  - $s \perp s'$.

Least Common Ancestor and Ting

- A set of states $S_1 \subseteq S$ is called **consistent**, denoted by $\downarrow S_1$, if and only if for each $s, s' \in S_1$,
  - $s \leq s'$,
  - $s' \leq s$, or
  - $s \perp s'$.



Legal Transitions

A hiearchical state-machine $(S, kind, region, \rightarrow, \psi, annot)$ is called **well-formed** if and only if for all transitions $t \in \rightarrow$,

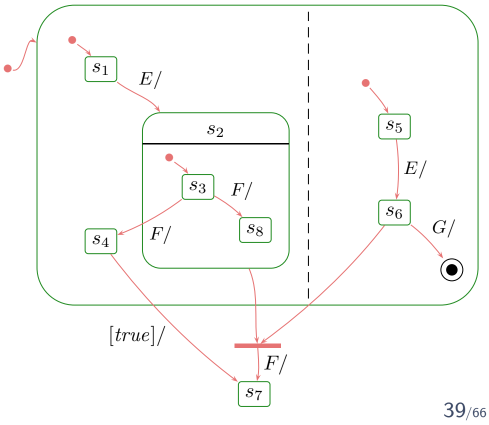
- source and destination are consistent, i.e. $\downarrow source(t)$ and $\downarrow target(t)$,
- source (and destination) states are pairwise unordered, i.e.
  - forall $s, s' \in source(t)$ $(\in target(t))$, $s \perp s'$,
- the top state is neither source nor destination, i.e.
  - $top \notin source(t) \cup source(t)$.
- Recall: final states are not sources of transitions.

Legal Transitions

A hiearchical state-machine $(S, kind, region, \rightarrow, \psi, annot)$ is called **well-formed** if and only if for all transitions $t \in \rightarrow$,

- source and destination are consistent, i.e. $\downarrow source(t)$ and $\downarrow target(t)$,
- source (and destination) states are pairwise unordered, i.e.
  - forall $s, s' \in source(t)$ $(\in target(t))$, $s \perp s'$,
- the top state is neither source nor destination, i.e.
  - $top \notin source(t) \cup source(t)$.
- Recall: final states are not sources of transitions.

Example:



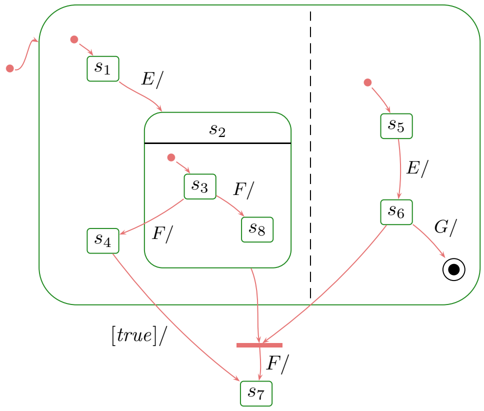
The Depth of States

- $depth(top) = 0$,
- $depth(s') = depth(s) + 1$, for all $s' \in child(s)$

The Depth of States

- $depth(top) = 0$,
- $depth(s') = depth(s) + 1$, for all $s' \in child(s)$

Example:



Enabledness in Hierarchical State-Machines

- The **scope** (“set of possibly affected states”) of a transition t is the **least common region** of
$$source(t) \cup target(t).$$

Enabledness in Hierarchical State-Machines

- The **scope** (“set of possibly affected states”) of a transition t is the **least common region** of
$$source(t) \cup target(t).$$

- Two transitions t_1, t_2 are called **consistent** if and only if their scopes are orthogonal (i.e. states in scopes pairwise orthogonal).

Enabledness in Hierarchical State-Machines

- The **scope** ("set of possibly affected states") of a transition t is the **least common region** of
$$source(t) \cup target(t).$$
- Two transitions t_1, t_2 are called **consistent** if and only if their scopes are orthogonal (i.e. states in scopes pairwise orthogonal).
- The **priority** of transition t is the depth of its innermost source state, i.e.
$$prio(t) := \max\{depth(s) \mid s \in source(t)\}$$

Enabledness in Hierarchical State-Machines

- The **scope** ("set of possibly affected states") of a transition t is the **least common region** of
$$source(t) \cup target(t).$$
- Two transitions t_1, t_2 are called **consistent** if and only if their scopes are orthogonal (i.e. states in scopes pairwise orthogonal).
- The **priority** of transition t is the depth of its innermost source state, i.e.
$$prio(t) := \max\{depth(s) \mid s \in source(t)\}$$

- A set of transitions $T \subseteq \rightarrow$ is **enabled** in an object u if and only if
  - T is consistent,
  - T is maximal wrt. priority,
  - all transitions in T share the same trigger,
  - all guards are satisfied by $\sigma(u)$, and
  - for all $t \in T$, the source states are active, i.e.
$$source(t) \subseteq \sigma(u)(st) \ (\subseteq S).$$

Transitions in Hierarchical State-Machines

- Let T be a set of transitions enabled in u.
- Then $(\sigma, \varepsilon) \xrightarrow{(cons, Snd)} (\sigma', \varepsilon')$ if
  - $\sigma'(u)(st)$ consists of the target states of t,

    i.e. for simple states the simple states themselves, for composite states the initial states,
  - σ', ε', $cons$, and Snd are the effect of firing each transition $t \in T$ **one by one**, **in any order**, i.e. for each $t \in T$,
    - the exit transformer of all affected states, highest depth first,
    - the transformer of t,
    - the entry transformer of all affected states, lowest depth first.

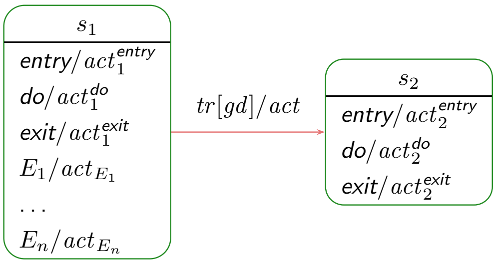
$\rightsquigarrow$ adjust (2.), (3.), (5.) accordingly.

Entry/Do/Exit Actions, Internal Transitions

Entry/Do/Exit Actions

- In general, with each state $s \in S$ there is associated
  - an **entry**, a **do**, and an **exit** action (default: skip)
  - a possibly empty set of trigger/action pairs called **internal transitions**,

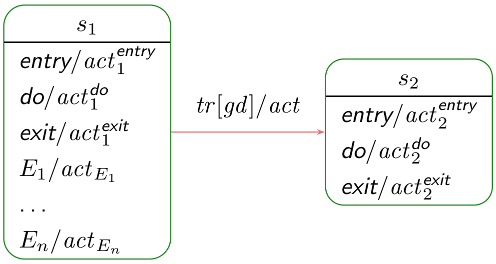
    (default: empty). $E_1, \dots, E_n \in \mathscr{E}$, 'entry', 'do', 'exit' are reserved names!



Entry/Do/Exit Actions

- In general, with each state $s \in S$ there is associated
  - an **entry**, a **do**, and an **exit** action (default: skip)
  - a possibly empty set of trigger/action pairs called **internal transitions**,

    (default: empty). $E_1, \dots, E_n \in \mathscr{E}$, 'entry', 'do', 'exit' are reserved names!



- Recall: each action's supposed to have a transformer. Here: $t_{act_1^{entry}}$, $t_{act_1^{exit}}$, ...
- Taking the transition above then amounts to applying

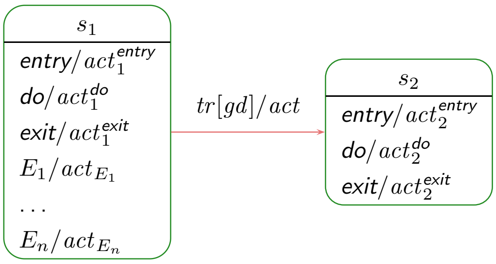
$$t_{act_{s_2}^{entry}} \circ t_{act} \circ t_{act_{s_1}^{exit}}$$

instead of only

$$t_{act}$$

$\rightsquigarrow$ adjust (2.), (3.) accordingly.

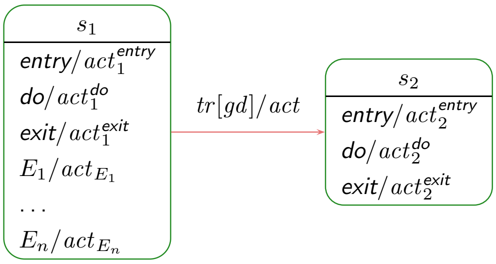
Internal Transitions



- For **internal transitions**, taking the one for E_1, for instance, still amounts to taking **only** $t_{act_{E_1}}$.
- Intuition: The state is neither left nor entered, so: no exit, no entry.

  $\rightsquigarrow$ adjust $(2.)$ accordingly.
- Note: internal transitions also start a run-to-completion step.

Internal Transitions



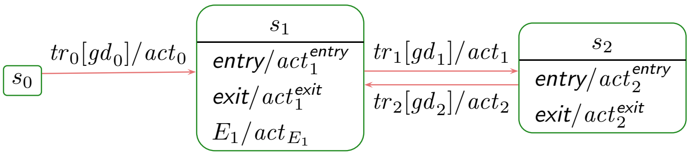
- For **internal transitions**, taking the one for E_1, for instance, still amounts to taking **only** $t_{act_{E_1}}$.
- Intuition: The state is neither left nor entered, so: no exit, no entry.

  $\rightsquigarrow$ adjust $(2.)$ accordingly.
- Note: internal transitions also start a run-to-completion step.

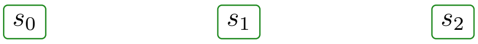
- Note: the standard seems not to clarify whether internal transitions have **priority** over regular transitions with the same trigger at the same state.

  Some code generators assume that internal transitions have priority!

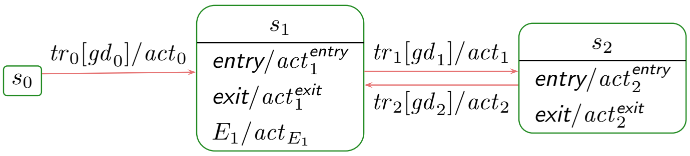
Alternative View: Entry/Exit/Internal as Abbreviations



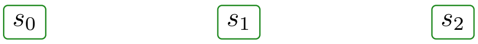
- ... as abbrevation for ...



Alternative View: Entry/Exit/Internal as Abbreviations

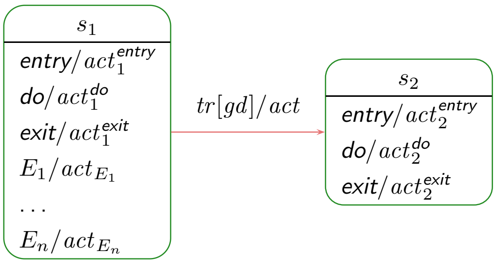


- ... as abbrevation for ...



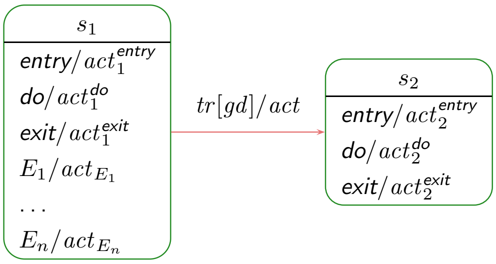
- That is: Entry/Internal/Exit don't add expressive power to Core State Machines. If internal actions should have priority, s_1 can be embedded into an OR-state (see later).
- Abbreviation may avoid confusion in context of hierarchical states (see later).

Do Actions



- **Intuition**: after entering a state, start its do-action.
- If the do-action terminates,
  - then the state is considered **completed**,
- otherwise,
  - if the state is left before termination, the do-action is stopped.

Do Actions



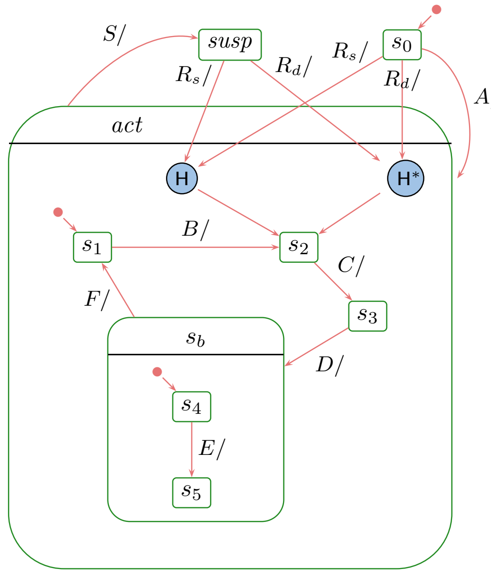
- **Intuition**: after entering a state, start its do-action.
- If the do-action terminates,
  - then the state is considered **completed**,
- otherwise,
  - if the state is left before termination, the do-action is stopped.

- Recall the overall UML State Machine philosophy:

  "An object is either idle or doing a run-to-completion step."
- Now, what is it exactly while the do action is executing...?

The Concept of History, and Other Pseudo-States

History and Deep History: By Example



What happens on...

- R_s?

  s_0, s_2

- R_d?

  s_0, s_2

- A, B, C, S, R_s?

  $s_0, s_1, s_2, s_3, susp, s_3$

- A, B, S, R_d?

  $s_0, s_1, s_2, s_3, susp, s_3$

- A, B, C, D, E, R_s?

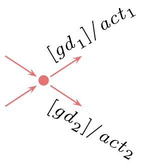
  $s_0, s_1, s_2, s_3, s_4, s_5, susp, s_3$

- A, B, C, D, R_d?

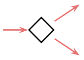
  $s_0, s_1, s_2, s_3, s_4, s_5, susp, s_5$

Junction and Choice

- Junction (**"static conditional branch"**):



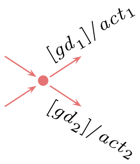
- Choice: (**"dynamic conditional branch"**)



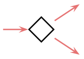
Note: not so sure about naming and symbols, e.g.,
I'd guessed it was just the other way round...

Junction and Choice

- Junction (**"static conditional branch"**):
  - **good**: abbreviation
  - unfolds to so many similar transitions with different guards, the unfolded transitions are then checked for enabledness
  - at best, start with trigger, branch into conditions, then apply actions

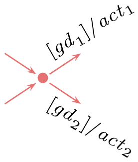


- Choice: (**"dynamic conditional branch"**)

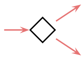


Note: not so sure about naming and symbols, e.g.,
I'd guessed it was just the other way round...

Junction and Choice



- Junction (**“static conditional branch”**):
  - **good**: abbreviation
  - unfolds to so many similar transitions with different guards, the unfolded transitions are then checked for enabledness
  - at best, start with trigger, branch into conditions, then apply actions

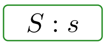


- Choice: (**“dynamic conditional branch”**)
  - **evil**: may get stuck
  - enters the transition **without knowing** whether there’s an enabled path
  - at best, use “else” and convince yourself that it cannot get stuck
  - maybe even better: **avoid**

Note: not so sure about naming and symbols, e.g.,
I’d guessed it was just the other way round...

Entry and Exit Point, Submachine State, Terminate

- Hierarchical states can be **“folded”** for readability.
  (but: this can also hinder readability.)
- Can even be taken from a different state-machine for re-use.



Entry and Exit Point, Submachine State, Terminate

- Hierarchical states can be **“folded”** for readability.
  (but: this can also hinder readability.)
- Can even be taken from a different state-machine for re-use. $\boxed{S : s}$
- **Entry/exit points** ○, ⊗
  - Provide connection points for finer integration into the current level, than just via initial state.
  - Semantically a bit tricky:
    - **First** the exit action of the exiting state,
    - **then** the actions of the transition,
    - **then** the entry actions of the entered state,
    - **then** action of the transition from
      the entry point to an internal state,
    - and **then** that internal state’s entry action.

Entry and Exit Point, Submachine State, Terminate

- Hierarchical states can be **“folded”** for readability.
  (but: this can also hinder readability.)
- Can even be taken from a different state-machine for re-use. $\boxed{S : s}$
- **Entry/exit points** ○, ⊗
  - Provide connection points for finer integration into the current level, than just via initial state.
  - Semantically a bit tricky:
    - **First** the exit action of the exiting state,
    - **then** the actions of the transition,
    - **then** the entry actions of the entered state,
    - **then** action of the transition from
      the entry point to an internal state,
    - and **then** that internal state’s entry action.

- **Terminate Pseudo-State** ×
  - When a terminate pseudo-state is reached,
    the object taking the transition is immediately killed.

Deferred Events in State-Machines

Active and Passive Objects [?]

What about non-Active Objects?

Recall:

- We're **still** working under the assumption that all classes in the class diagram (and thus all objects) are **active**.
- That is, each object has its own thread of control and is (if stable) at any time ready to process an event from the ether.

What about non-Active Objects?

Recall:

- We're **still** working under the assumption that all classes in the class diagram (and thus all objects) are **active**.
- That is, each object has its own thread of control and is (if stable) at any time ready to process an event from the ether.

But the world doesn't consist of only active objects.

For instance, in the crossing controller from the exercises we could wish to have the whole system live in one thread of control.

So we have to address questions like:

- Can we send events to a non-active object?
- And if so, when are these events processed?
- etc.

Active and Passive Objects: Nomenclature

[?] propose the following (orthogonal!) notions:

- A class (and thus the instances of this class) is either **active** or **passive** as declared in the class diagram.
  - An **active** object has (in the operating system sense) an own thread: an own program counter, an own stack, etc.
  - A **passive** object doesn't.

Active and Passive Objects: Nomenclature

[?] propose the following (orthogonal!) notions:

- A class (and thus the instances of this class) is either **active** or **passive** as declared in the class diagram.
  - An **active** object has (in the operating system sense) an own thread: an own program counter, an own stack, etc.
  - A **passive** object doesn't.

- A class is either **reactive** or **non-reactive**.
  - A **reactive** class has a (non-trivial) state machine.
  - A **non-reactive** one hasn't.

Active and Passive Objects: Nomenclature

[?] propose the following (orthogonal!) notions:

- A class (and thus the instances of this class) is either **active** or **passive** as declared in the class diagram.
  - An **active** object has (in the operating system sense) an own thread: an own program counter, an own stack, etc.
  - A **passive** object doesn't.
- A class is either **reactive** or **non-reactive**.
  - A **reactive** class has a (non-trivial) state machine.
  - A **non-reactive** one hasn't.

Which combinations do we understand?

	active	passive
reactive	✔	(∗)
non-reactive	(✔)	(✔)

Passive and Reactive

- So why don't we understand passive/reactive?
- Assume passive objects u_1 and u_2, and active object u, and that there are events in the ether for all three.

  Which of them (can) start a run-to-completion step...?
  Do run-to-completion steps still interleave...?

Passive and Reactive

- So why don't we understand passive/reactive?
- Assume passive objects u_1 and u_2, and active object u, and that there are events in the ether for all three.

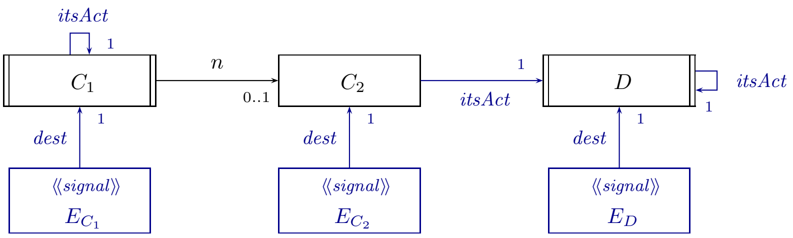
  Which of them (can) start a run-to-completion step...?
  Do run-to-completion steps still interleave...?

Reasonable Approaches:

- **Avoid** — for instance, by
  - require that **reactive implies active** for model well-formedness.
  - requiring for model well-formedness that events are **never sent** to instances of non-reactive classes.
- **Explain** — here: (following [?])
  - Delegate all dispatching of events to the active objects.

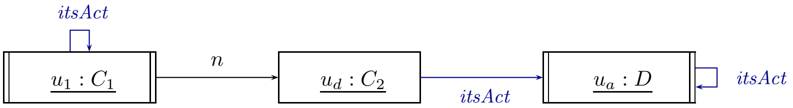
Passive Reactive Classes

- Firstly, establish that each object u knows, via (implicit) link $itsAct$, **the active object** u_{act} which is responsible for dispatching events to u.
- If u is an instance of an active class, then $u_a = u$.



Passive Reactive Classes

- Firstly, establish that each object u knows, via (implicit) link $itsAct$, **the active object** u_{act} which is responsible for dispatching events to u.
- If u is an instance of an active class, then $u_a = u$.

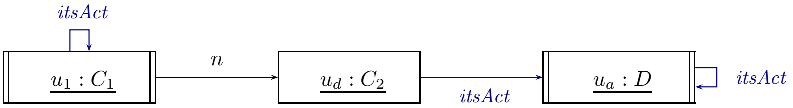


Sending an event:

- Establish that of each signal we have a version E_C with an association $dest : C_{0,1}$, $C \in \mathscr{C}$.
- Then $n!E$ in $u_1 : C_1$ becomes:
- Create an instance u_e of E_{C_2} and set u_e's $dest$ to $u_d := \sigma(u_1)(n)$.
- Send to $u_a := \sigma(\sigma(u_1)(n))(itsAct)$, i.e., $\varepsilon' = \varepsilon \oplus (u_a, u_e)$.

Passive Reactive Classes

- Firstly, establish that each object u knows, via (implicit) link $itsAct$, **the active object** u_{act} which is responsible for dispatching events to u.
- If u is an instance of an active class, then $u_a = u$.



Sending an event:

- Establish that of each signal we have a version E_C with an association $dest : C_{0,1}$, $C \in \mathscr{C}$.
- Then $n!E$ in $u_1 : C_1$ becomes:
- Create an instance u_e of E_{C_2} and set u_e's $dest$ to $u_d := \sigma(u_1)(n)$.
- Send to $u_a := \sigma(\sigma(u_1)(n))(itsAct)$, i.e., $\varepsilon' = \varepsilon \oplus (u_a, u_e)$.

Dispatching an event:

- Observation: the ether only has events for active objects.
- Say u_e is ready in the ether for u_a.
- Then u_a asks $\sigma(u_e)(dest) = u_d$ to process u_e — and waits until completion of corresponding RTC.
- u_d may in particular discard event.

And What About Methods?

And What About Methods?

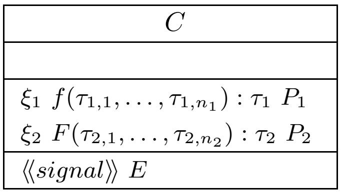
- In the current setting, the (local) state of objects is only modified by actions of transitions, which we abstract to transformers.
- In general, there are also **methods**.
- UML follows an approach to separate
  - the **interface declaration** from
  - the **implementation**.

  In C++ lingo: distinguish **declaration** and **definition** of method.

And What About Methods?

- In the current setting, the (local) state of objects is only modified by actions of transitions, which we abstract to transformers.
- In general, there are also **methods**.
- UML follows an approach to separate
  - the **interface declaration** from
  - the **implementation**.

  In C++ lingo: distinguish **declaration** and **definition** of method.



C

$\xi_1\ f(\tau_{1,1},\dots,\tau_{1,n_1}) : \tau_1\ P_1$

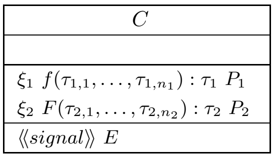
$\xi_2\ F(\tau_{2,1},\dots,\tau_{2,n_2}) : \tau_2\ P_2$

$\langle\langle signal \rangle\rangle\ E$

- In UML, the former is called **behavioural feature** and can (roughly) be
  - a **call interface** $f(\tau_{1_1},\dots,\tau_{n_1}) : \tau_1$
  - a **signal name** E

  Note: The signal list is redundant as it can be looked up in the state machine of the class. But: certainly useful for documentation.

Behavioural Features



C

$\xi_1\ f(\tau_{1,1},\dots,\tau_{1,n_1}) : \tau_1\ P_1$

$\xi_2\ F(\tau_{2,1},\dots,\tau_{2,n_2}) : \tau_2\ P_2$

$\langle\langle signal \rangle\rangle\ E$

Semantics:

- The **implementation** of a behavioural feature can be provided by:
  - An **operation**.
  - The class' **state-machine** ("triggered operation").

Behavioural Features

C
$\xi_1\ f(\tau_{1,1},\dots,\tau_{1,n_1}) : \tau_1\ P_1$ $\xi_2\ F(\tau_{2,1},\dots,\tau_{2,n_2}) : \tau_2\ P_2$
$\langle\langle signal\rangle\rangle\ E$

Semantics:

- The **implementation** of a behavioural feature can be provided by:
  - An **operation**.

    In our setting, we simply assume a transformer like T_f.

    It is then, e.g. clear how to admit method calls as actions on transitions: function composition of transformers (clear but tedious: non-termination).

    In a setting with Java as action language: operation is a method body.
  - The class' **state-machine** ("triggered operation").

Behavioural Features

C
$\xi_1\ f(\tau_{1,1},\dots,\tau_{1,n_1}) : \tau_1\ P_1$ $\xi_2\ F(\tau_{2,1},\dots,\tau_{2,n_2}) : \tau_2\ P_2$
$\langle\langle signal\rangle\rangle\ E$

Semantics:

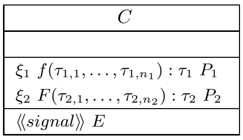
- The **implementation** of a behavioural feature can be provided by:
  - An **operation**.

    In our setting, we simply assume a transformer like T_f.

    It is then, e.g. clear how to admit method calls as actions on transitions: function composition of transformers (clear but tedious: non-termination).

    In a setting with Java as action language: operation is a method body.
  - The class' **state-machine** ("triggered operation").
    - Calling F with n_2 parameters for a stable instance of C creates an auxiliary event F and dispatches it (bypassing the ether).
    - Transition actions may fill in the return value.
    - On completion of the RTC step, the call returns.
    - For a non-stable instance, the caller blocks until stability is reached again.

Behavioural Features: Visibility and Properties



C

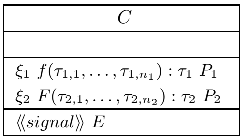
$\xi_1\ f(\tau_{1,1},\dots,\tau_{1,n_1}) : \tau_1\ P_1$

$\xi_2\ F(\tau_{2,1},\dots,\tau_{2,n_2}) : \tau_2\ P_2$

$\langle\langle signal\rangle\rangle\ E$

- **Visibility**:
  - Extend typing rules to sequences of actions such that a well-typed action sequence only calls visible methods.

Behavioural Features: Visibility and Properties



C

$\xi_1\ f(\tau_{1,1},\dots,\tau_{1,n_1}) : \tau_1\ P_1$

$\xi_2\ F(\tau_{2,1},\dots,\tau_{2,n_2}) : \tau_2\ P_2$

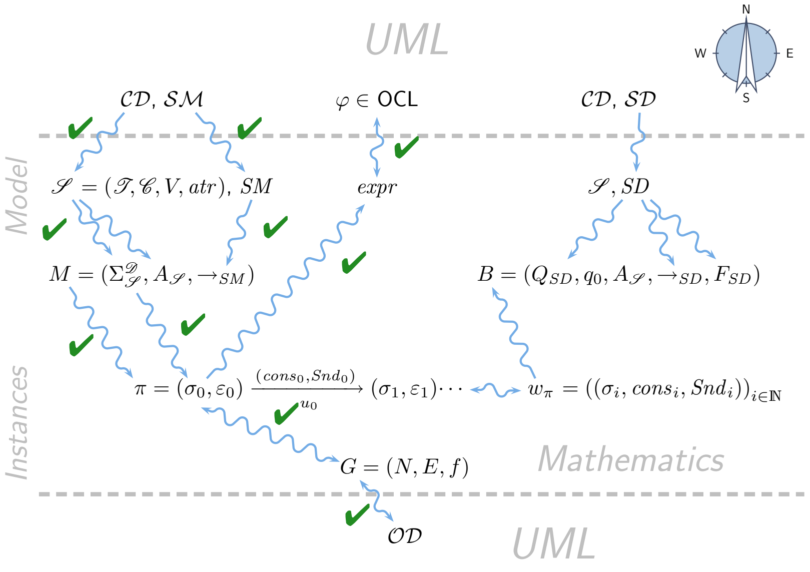
$\langle\langle signal\rangle\rangle\ E$

- **Visibility**:
  - Extend typing rules to sequences of actions such that a well-typed action sequence only calls visible methods.
- **Useful properties**:
  - **concurrency**
    - **concurrent** — is thread safe
    - **guarded** — some mechanism ensures/should ensure mutual exclusion
    - **sequential** — is not thread safe, users have to ensure mutual exclusion
  - **isQuery** — doesn't modify the state space (thus thread safe)
- For simplicity, we leave the notion of steps untouched, we construct our semantics around state machines.
  Yet we could explain pre/post in OCL (if we wanted to).

Discussion.

You are here.

Course Map



UML

$\mathcal{CD}$, $\mathcal{SM}$

$\varphi \in$ OCL

$\mathcal{CD}$, $\mathcal{SD}$

Model

$\mathscr{S} = (\mathscr{T}, \mathscr{C}, V, atr)$, SM

$expr$

$\mathscr{S}, SD$

$M = (\Sigma_{\mathscr{S}}^{\mathscr{D}}, A_{\mathscr{S}}, \rightarrow_{SM})$

$B = (Q_{SD}, q_0, A_{\mathscr{S}}, \rightarrow_{SD}, F_{SD})$

Instances

$\pi = (\sigma_0, \varepsilon_0) \xrightarrow[u_0]{(cons_0, Snd_0)} (\sigma_1, \varepsilon_1) \cdots$

$w_\pi = ((\sigma_i, cons_i, Snd_i))_{i \in \mathbb{N}}$

$G = (N, E, f)$

Mathematics

$\mathcal{OD}$

UML

References